

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#5

Inventor: Gregg B. Morrison)

Serial No. 09/773,487)

Filed: February 2, 2001)

For: Processes and Systems for Enabling Secure)
And Controlled Distribution and Use of)
Information)

Petition to Make

Special Under

37 CFR 1.102(d)

Hon. Commissioner of Patents
and Trademarks
Box PCT
Washington, D.C. 20231

RECEIVED
FEB 06 2003
Technology Center 2100

Sir:

Applicant requests to make the above-identified application special according to the provision set forth in 37 CFR 1.102(d). A required fee of \$130.00 is enclosed. It is not believed that any other fee is required for the purpose of making the application special; however, the Commissioner is authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. 50-1682.

Statement Explaining How the Invention Contributes to Countering Terrorism

The forensic methods described in the above-identified application are employed to positively identify an object--either software or hardware--by means of specific measurements in quantifiable and repeatable terms, and to such a level of detail as is required to detect any attempt to falsify the measurement.

This forensic measurement is singular to the object that was measured to a level that positively identifies the specific object from any other similar object. The measurement can be employed as a unique identifier for the specific object.

10/11/2002 MKAYPAGH 00000069 09773487

01 FC:154

130.00 DP

Any electronic equipment that features either processing capability or a method of data exchange, such as a personal computer ("PC"), cellular phone, or other device, can be positively identified using the methods described. Various identifying information can be obtained from sources in the hardware that will positively identify any PC, for example, and tell it apart from every other PC--even those made by the same manufacturer and containing the same make and model components. Similar identifying information can be obtained from cellular phones and many other devices.

Typical PC identifiers are not unique and specific and are too generic to be used to establish an absolute identifier. Therefore it is necessary to deeply probe (mine) the hardware to obtain a unique identifier for any given personal computer. This mining is necessary because most systems isolate the operating system from the hardware by drivers and security layers that hide operational and hardware details. Any application can call a forensic probe function expect standard results. When mining for specifically unique identifiers in any computer system, the obvious components or data must be ignored in favor of those unique identifiers that have the best opportunity to survive the life of the system. Any component that is likely to be upgraded during the life of the system should not be used. For example, a system board itself is subject to upgrades.

The most reliable components for extracting singular and unique identifiers are those which are too costly, too important, too risky, too inconvenient, or too complicated for the user to replace, or components which the user does not normally find reason to replace. The two leading components in a common PC are the main system hard drive and, if installed, any network cards. Other information is available from the electronics of every hard drive, such as the 20-plus digit serial number that the manufacturer has printed on the drive label, and that is commonly used to identify a drive under warranty. This information is stored in chips on the drive and cannot be altered by the user in any way. Even a disk that is inoperable, magnetized, dropped, crashed or otherwise unusable will maintain this signature data, provided the chips remain intact. Even when a lightning strike or an electrical power surge destroys a computer system, in most cases the hard drive identity in these chips actually survives.

The hard drive forensic signature can be as simple as reading the data, splitting it, and taking a Cyclic Redundancy Check of each half to obtain an inalterable and highly survivable 128-bit Forensic Identifier.

Any data can be specifically protected through various methods of apply the forensic identity of the device itself, especially by encryption or enciphering of the data, or through a forensic identity enabling mechanism, such as could be used to apply a license or user enforcement mechanism.

The result is that data can be made available only to specifically authorized PCs or other devices, specific users, or specific locations, so that other unauthorized PCs or other devices cannot access the protected data. Databases can be protected from hacking; and software can be designated to operate only on authorized PCs. Communications can be sealed against any compromise by including the specific forensic device identity into part of an encryption or enciphering scheme.

Application of the Technology to Countering Terrorism

Law enforcement, other government agencies, the military, and private industry have grown increasingly concerned that our computer systems and data files are not secure from infiltration and interference by electronic terrorist activity. The Office of Homeland Security has identified a number of areas in which electronic security must be improved. The technology described above can be highly useful in the following ways, among others:

- (1) Secure sharing of law enforcement data files. Published reports indicate that federal officials want to establish better links between local, state, and federal law enforcement to share data files concerning potential terrorist activity. It has become apparent that the events of September 11 might have been prevented with better communication of investigative information in the months preceding the attack. The technology described above can be used to establish secure links between authorized PCs to access national databases of information. The technology can streamline access to the information and also protect the information from unauthorized access.

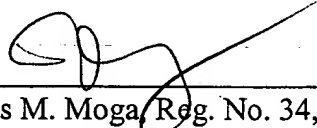
- (2) Secure communication of information to and from the field. Satellite links used for transmission of satellite photos of Afghanistan, for example, are reportedly subject to interception. If that is the case, other transmitted information regarding Iraq and other anti-terrorist data is also not secure. It has been reported that satellite data regarding Afghanistan has been downloaded in the United States, sent by military courier to Europe, and driven to Afghanistan for use by our military on the ground, because electronic delivery of the information is not secure. The technology described above can be used to establish a secure transmission of data to any designated PC in any location in the world, with no potential for interception of the data. Similarly, it can allow U.S. military operating in hostile territory to communicate securely with their command centers, without interception of the transmitted information.
- (3) Secure transmission of airport security information. Steps are underway to develop systems to screen and identify passengers and baggage in all airports. However, the information gathered at the passenger check-in and at other points during the boarding process is not linked in a secure fashion. The technology can supplement existing and future security measures by preventing any hacking into or alteration of the digital data after it is gathered.
- (4) Protection of business and financial data. Officials have stated publicly their concern that one fertile ground for terrorist activity is the potential destruction of business and financial data necessary for the normal, day-to-day operation of the United States economy. Knowledgeable hackers in remote locations around the world attempt every day to gain access to important governmental and industry data files. The technology described above can be employed to improve security of such data and prevent terrorist access to such information.

As discussed above, it is believed that the present invention can significantly contribute to counter terrorism. Favorable and prompt consideration is respectfully requested.

Date:

9 Oct 02

By:



Thomas M. Moga, Reg. No. 34,881
Attorney for the Applicants

POWELL, GOLDSTEIN, FRAZER & MURPHY LLP
P.O. Box 97223
Washington, D.C. 20090-7223
(202) 347-0066

TM/SL/dp